elaman
German Security Solutions

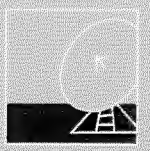
# GOVERNMENTAL SECURITY SOLUTIONS

## COMMUNICATIONS MONITORING SOLUTIONS

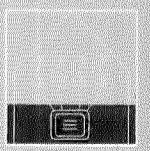

6


6


7

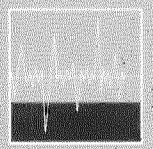

8


9

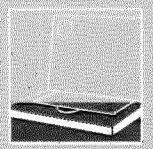

10

# CONTENT

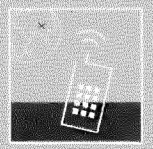




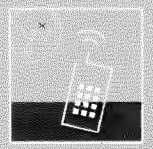




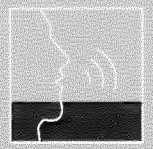


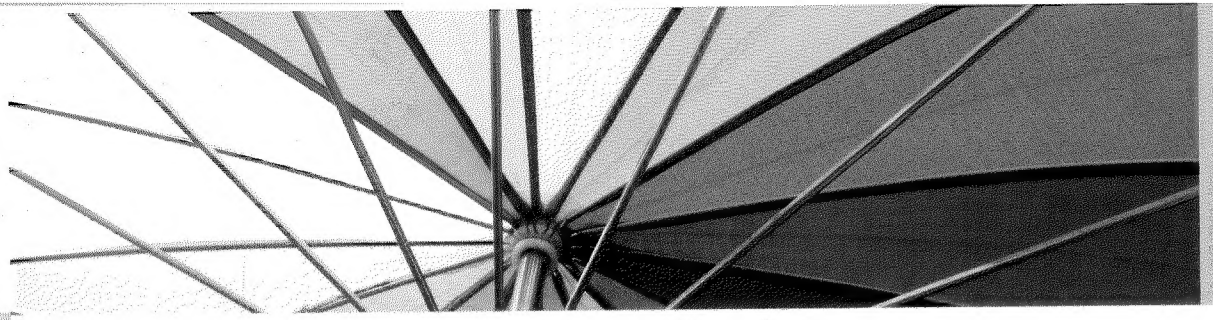




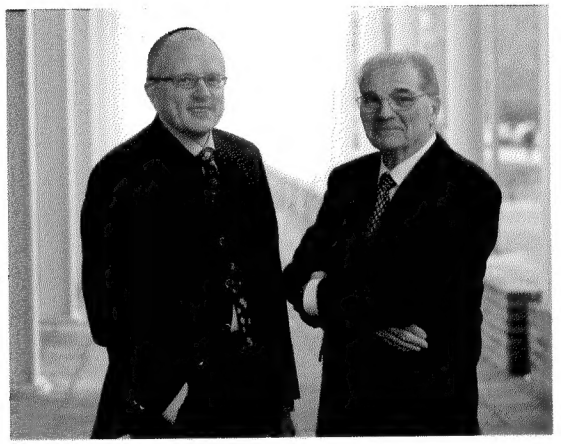








# COMMUNICATIONS MONITORING SOLUTIONS FROM ELAMAN



Managing Director Holger Rumscheidt with his Partner and Senior Consultant Eugen Fissl.

Elaman is a German based company that was established in 2004 and has its headquarters in Munich, Germany.

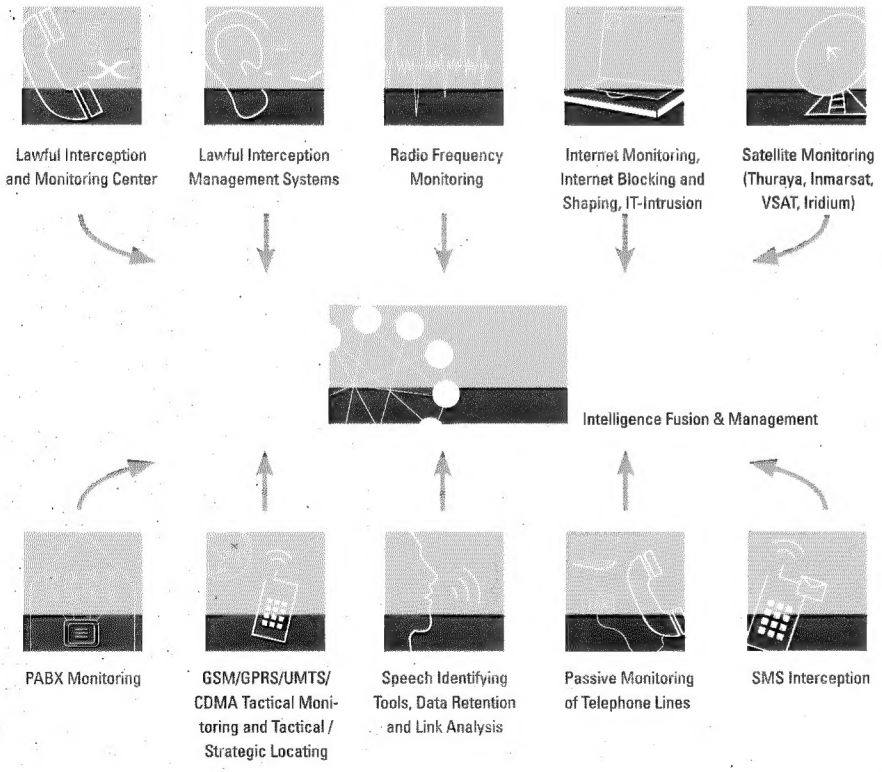
Our aim is to provide comprehensive security products and solutions, technical consultancy and services as well as professional training for governments and security agencies.

The common aim of all Law Enforcement Agencies is to have state of the art capabilities to intercept all kinds of communications within different telecommunications networks and carriers inside and outside a country's borders. Different methods of communications exist, such as network based communications (PSTN), Internet, private networks (PABX), wireless communications (WIFI, WIMAX, etc.), cellular communications (GSM/GPRS/UMTS/CDMA) and satellite communications (Thuraya, Inmarsat, VSAT, Iridium, etc.).

For all these technologies, different intercept systems are available from huge strategic systems to small portable tactical units:

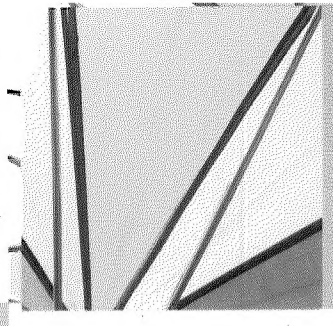
- Lawful Interception and Monitoring Centers
- Lawful Interception Management Systems (LIMS)
- Radio Frequency Monitoring
- Internet Monitoring, Internet Blocking and Shaping, IT-Intrusion
- Satellite Monitoring (Thuraya, Inmarsat, VSAT, Iridium, etc.)
- PABX Monitoring
- GSM/GPRS/UMTS/CDMA Tactical Monitoring and Tactical and Strategic Locating
- Speech Identifying Tools, Data Retention and Link Analysis
- Passive Monitoring of Telephone Lines
- SMS Interception

**> Intelligence Fusion & Management**
**> Technical Consultancy for Communications Monitoring**

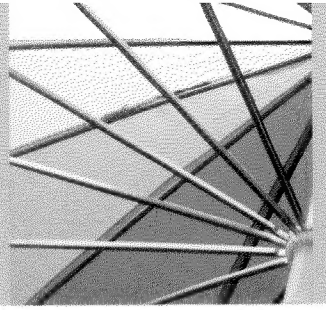



Technical Consultancy for Communications Monitoring

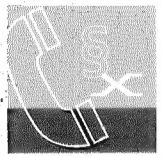
Elaman provides solutions in all fields and can be the sole supplier and technical consultant for such systems. Our combination of developments and systems, using third party products and integrating different systems, enables Elaman, as a sole supplier, to provide our clients with a unique portfolio of the best services and solutions on the market. With such a setup we are able to discuss possible interfacing between Monitoring Systems having one common platform in place for data collection and analysis (Intelligence Fusion & Management). Elaman's Technical Consultancy for Communications Monitoring is a service that provides our clients with an "umbrella" of all systems and solutions in this field from the process of setting requirements, tendering, ordering, implementing and operation.



## LAWFUL INTERCEPTION OF PSTN / GSM /UMTS ETC. NETWORKS AND MONITORING CENTER



## LAWFUL INTERCEPTION MANAGEMENT SYSTEMS (LIMS)



Lawful Interception (LI) is the legally approved interception of telecommunications networks and has become an important tool for Law Enforcement Agencies (LEAs) around the world. Lawful Interception provides access to calls and call-related information (telephone numbers, date, time, etc.) within telecommunications networks, and delivers this data to a strategic Monitoring Center (MC). The MC can decode, store and playback/view the data (call, data, fax). The interface between the MC and the telecommunications networks varies depending on the networks (PSTN, GSM, GPRS, UMTS, CDMA, IP, etc.) and the switches used (Nokia Siemens Networks, Ericsson, Huawei, Alcatel-Lucent, Cisco, Juniper, etc.). Such an MC gives access to an entire country's telecommunications network from one central place, but it needs the support of operators and the relevant interception capabilities of the network elements (Hardware and Software).

The LIMS solution usually acts as a bridge or mediator between the telecommunications operators and Law Enforcement Agencies using Monitoring Center solutions for PSTN, GSM, GPRS, UMTS, CDMA, IP, etc. The LIMS solution can provide interfaces for all kinds of network elements. It will standardize the interface back to the Monitoring Center to provide a homogeneous structure of the Monitoring Center under one generic Graphical User Interface. Umbrella LIMS solutions are available to act as the only administration terminal to mark phone numbers within different kinds of networks from different vendors and operators.

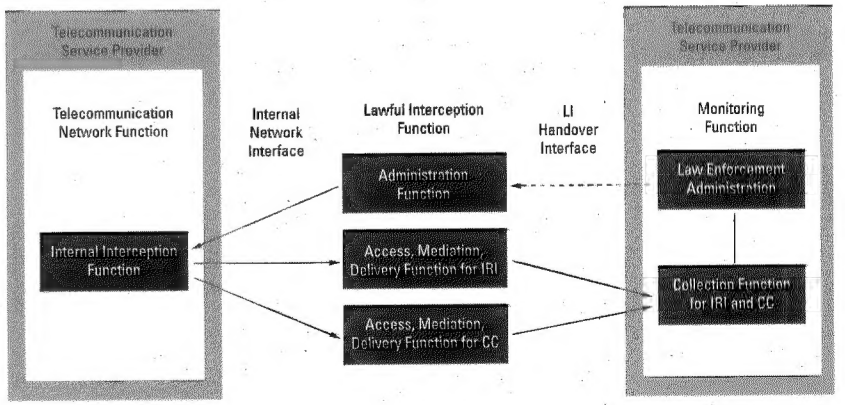
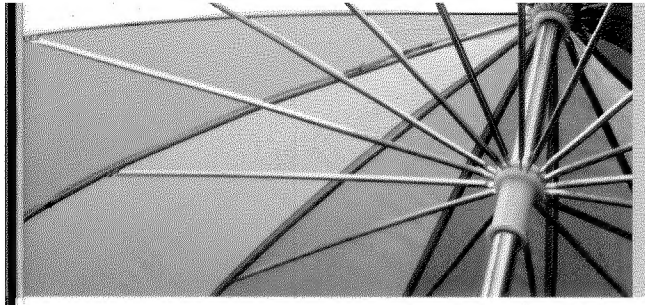
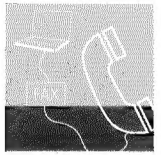



Figure 1. Functional model for lawful interception



# PASSIVE MONITORING OF TELEPHONE LINES



The possibility to passively monitor a huge number of telephone lines has become more and more important as it provides a full history of telephone data for a predefined time-frame (e.g. last six month).

In this case, all communications are passively intercepted without active intervention by the communications network. This is an ideal method to collect information for intelligence agencies, and also to identify targets for use in a Lawful Interception (LI) based system. The number of intercepts in the case of passive Interception is much larger than in the case of LI.

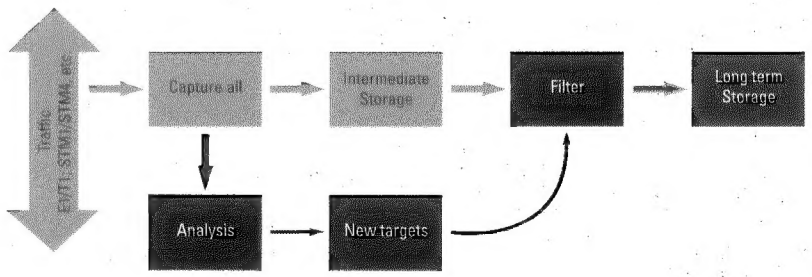
The aim of passive surveillance is to intercept all traffic (voice, faxes, data-sessions, emails, internet sessions, etc.) on:

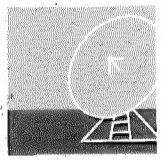
**International gateways:**
This point provides all land-based communication across the borders of a country. The same technology can equally be used to intercept within the country or in a specific area.

**Mobile Networks (PLMN)**
From a passive perspective, this is the interception between PSTN and PLMN as well as within PLMN systems themselves on the level of the communications between the MSC and BSC.

**The demands of passive surveillance are:**

- **Large volumes of traffic need to be intercepted (e.g. 1000s of E1s)**
- **Different types of interfaces are required (E1/T1; STM1/STM4, etc.)**
- **Large storage capacity (Petabytes) and vast processing & filtering are required**
- **Changes in protocols or telecommunication environments continue to occur**





First, it is important to distinguish between the two types of satellite systems concepts:

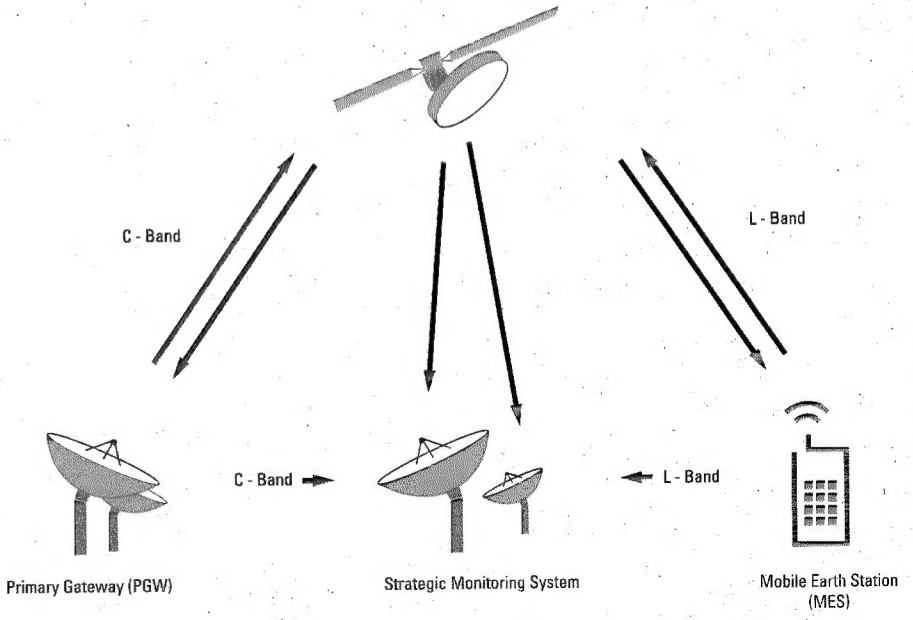
- **General satellite operators, like EutelSat, ArabSat, IntelSat, etc. are mainly used to provide telecoms carriers or broadcasting stations with a transmission bandwidth or provide dedicated links to private users and organizations (VSat)**

- **Satellite communications systems provide clients with communication services over certain providers, like Inmarsat, Thuraya, Iridium, etc., using attractive handhelds similar to GSM phones**

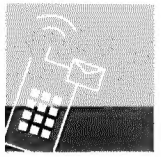
The approach to define an interception capability is totally different for both types. For general Satellite Systems a detailed survey is required, as the interception solution will be different for each country based on the satellite footprints and the terminals used within the area that should be intercepted.

For satellite communication – "off the shelf" interception systems are available. These systems are purely passive and do not need any support from a satellite operator. All signals are passively monitored, decoded and viewed. In case of Thuraya Monitoring, the exact positions of the intercepted phones will also be given.

Satellite interception, especially with the Thuraya network, is becoming more and more important as mobile satellite services have expanded very successfully due to the small size of handhelds and the combined roaming possibilities within the GSM networks using the same handset. The coverage of Inmarsat is worldwide. The coverage of Thuraya is over Europe, Middle East, most of Africa, Central Asia, Far East and Australia.

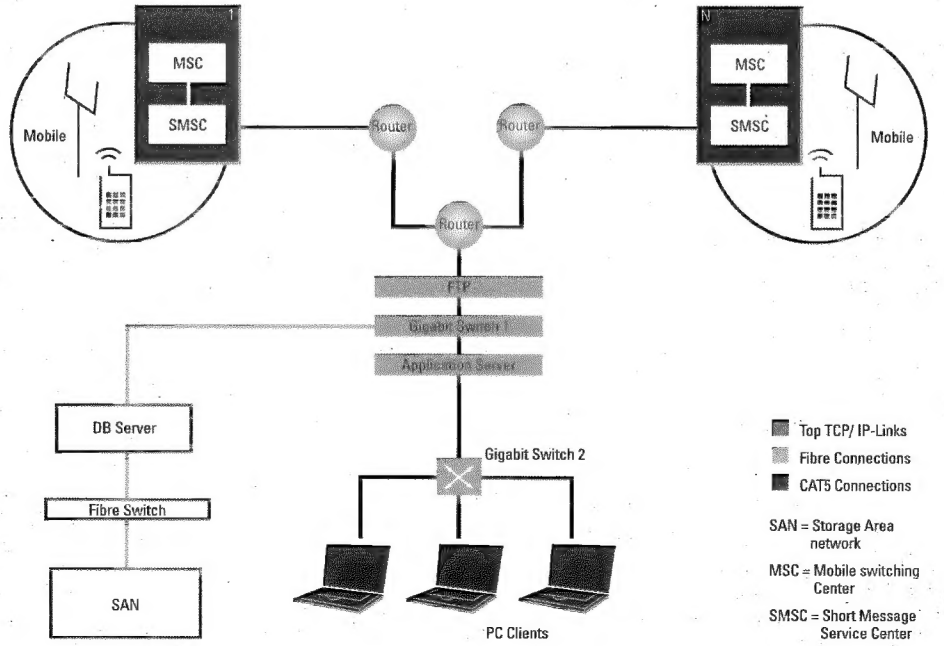


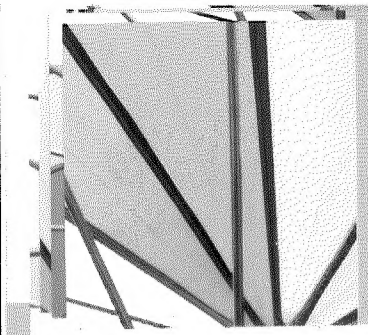
# SMS INTERCEPTION



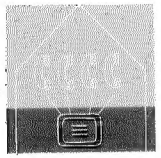
The SMS interception system is connected to the GSM operators Short Message Service Centre (SMSC) within a Mobile Switching Centre (MSC) and receives all SMS. The system decodes, monitors, and stores them via the secure TCP/IP connections. All SMS are inserted into a central database for later analysis.

The system is capable of holding multibillions of records over terabytes of storage systems and can process up to 200 million SMS' per day. By implementing the latest database technologies the system offers long-term archiving of SMS and fast data mining capabilities, including a full indexed multilingual SMS text-search. The implementation and interfacing of an SMS interception system depends on the type and version of the operator's Short Message Service Center (SMSC). The modular configuration of the SMS interception system allows it to interface and adapt to each vendor of such SMSC.

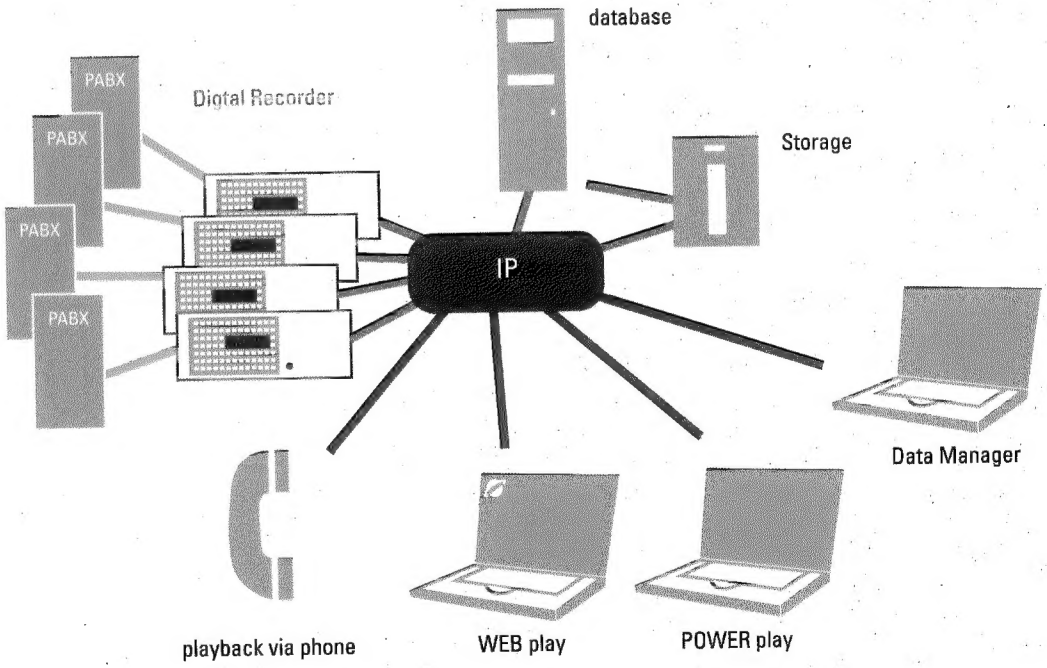




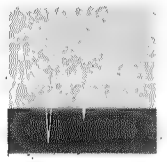




A strategic LI monitoring system can intercept all communications within an operator's communications network (e.g. PSTN, GSM, UMTS, CDMA, etc.). Such a system does not offer the ability to monitor calls, faxes and data within private networks (PABX of hotels, companies, etc.). Based on the type of PABX, a variety of interception solutions are possible. For instance, equipment must be installed in the PABX in order to have access to a private network to mark certain numbers to be intercepted (extension) and to route intercepted calls to a place where the recording and storage should be done. Remote control is possible, particularly for network wide recording solutions in case several PABXs are connected to a communication network. A PABX interception solution can also be integrated into LI-Monitoring Systems in order to use a single platform and give the operator one common Graphical User Interface.



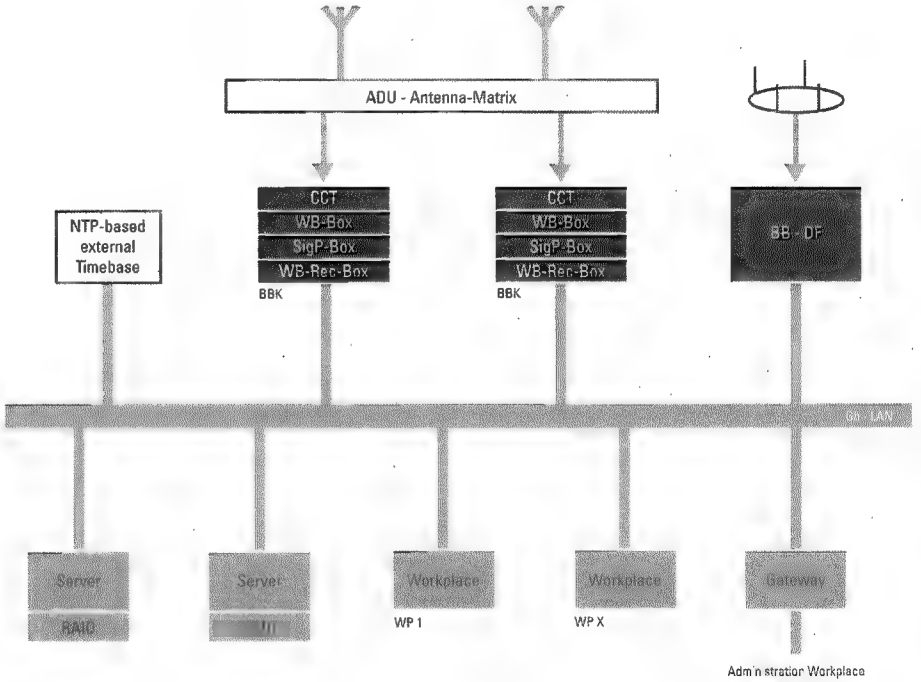

PABX: Private Automatic Branch Exchange



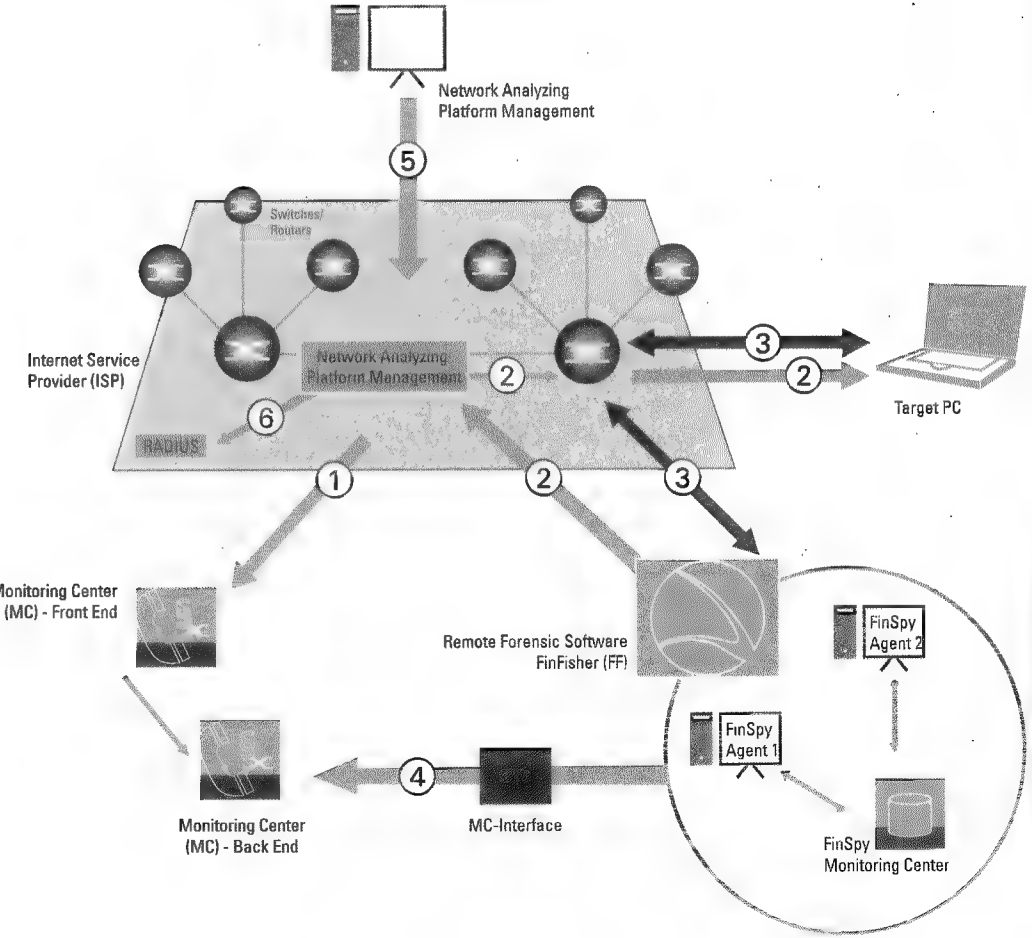
Telecom Regulatory Authorities need Radio Frequency (RF) Monitoring systems based on ITU recommendations and systems to monitor their target/client if they follow their license agreements and ITU standards. The key for Law Enforcement Agencies is to have access to the content of Radio Frequency Signals and to locate them. Therefore, the focus is on:

- **Signal Detection**
- **Signal Classification**
- **Signal Analysis**
- **Signal Decoding/ Demodulating**
- **Wideband Recording**
- **Direction Finding Systems**
- **Speech Classification**

The design, production and delivery of systems on turnkey bases are essential and the use of COTS (Commercial Off The Shelf) technology makes the operation of the system easier and extremely cost effective. A wide range of RF-Monitoring systems can be offered from big strategic systems to portable tactical systems including Direction Finding Systems.

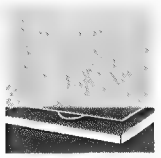



| | | | |
|---|---|---|---|
| **ADU** | Antenna Distribution Unit | **WB Rec Box** | Wideband Recording Box |
| **CCT** | ComCat Tuner | **BB DF** | BroadBand Direction Finding |
| **WB Box** | Wideband Box | **BBK** | Broad Band Component |
| **SigP Box** | Signal Processing Box | | |




1. Passive intercept of all IP-Data which goes via ISP backbone
   Filtering - Decoding - Storage - Viewing: Target Based Interception & „wild card" based
2. Active injection of FinSpy to target PC
3. Remote control of target PC: Full interception of all data of target PC (Http, Mail, Skype, VoIP etc.)
4. FinFisher Interface
5. IP Manipulation (blocking of IP-traffic & shaping)
6. RADIUS - Monitoring Correlation (TCP/IP address login)

# FINFISHER: GOVERNMENTAL IT INTRUSION AND REMOTE MONITORING SOLUTIONS



FinFisher is the leading offensive IT Intrusion solution through which Elaman provides complementary solutions, products and advanced training capabilities to Government end-users who are seeking world class offensive techniques for information gathering from suspects and targets.

FinFisher combines three critical areas in one comprehensive IT Intrusion Portfolio giving the Law Enforcement and Intelligence Communities a vast array of intrusion capabilities from starting up a new Intrusion Department to providing world-class solutions and training for enhancing existing resources.

### [illegible] & Infection

FinSpy is a product used for remote monitoring and real-time access to target systems, allowing access even to encrypted data and communications. In combination with enhanced remote infection methods, which fall under the FinFly family of products, the end-user will have the capability to remotely infect a target's Windows or OSX based PC. In addition to target computer systems, FinSpy Mobile allows monitoring of Symbian, Blackberry, iPhone, Windows Mobile Devices, Android and Maemo.

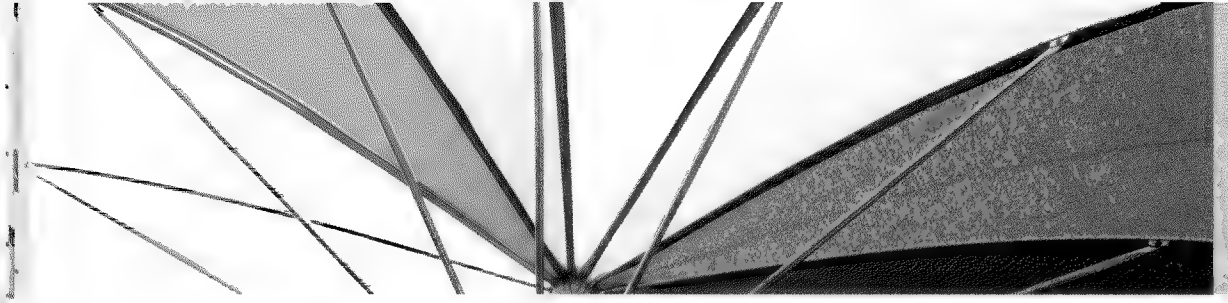
### factical IT Intrusion Portfolio.

Having the right set of tools enables the agencies to maximize the use of their resources. The FinIntrusion Kit provides end-users with the needed know-how and capabilities to optimize operations as well as significantly increasing their success rate. With the upcoming introduction of FinFireWire, end-users will be able to access Windows, OSX & Linux-based systems via the FireWire port, PCMCIA or Express card without the need for any logon information.

### IT Intrusion Training Program

The use of all our solutions can be maximized depending on the end-user's knowledge of the offensive IT Field. Therefore, Elaman provides extensive training courses both on products supplied as well as practical IT Intrusion methods and techniques, transferring years of knowledge and experience to end-users and thus maximizing their capabilities in this field.

FINFISHER
IT INTRUSION





For operational field usage, off-air GSM monitoring systems are very powerful and essential. Such systems are portable and can be installed into vehicles for covert operations. Systems for GSM, GPRS, UMTS and CDMA are available. Three different types are available:

### Active systems

Such systems simulate a GSM/UMTS base station to attract GSM/UMTS phones away from the normal GSM/UMTS network and log into the system´s "fake" virtual base station. As soon as the phone is logged onto the more attractive active system, its identity is extracted (IMSI and IMEI). By logging the phone onto the virtual base station the phone can be forced to transmit on a given channel, frequency and time-slot (establishing a "silent call"). This transmission can be picked up by a direction finding system (vehicle based or handheld) which then gives the exact position of the target phone. When the target phone is logged into the active system intercepting of calls can be done, but only calls that are initiated by the target (target is out of the normal GSM/UMTS network so no calls can be received by the target phone). In addition, phones can be completely taken off the real network ("intelligent jamming"), fake calls and SMS can be sent to the target phone, and private networking by using the virtual base station can be realized and the battery of the target phone can be drained, etc. The active system also allows operating within UMTS networks. Collecting the identity of the target phone (IMSI, IMEI) can be done without bringing the phone down to GSM/GPRS, therefore, no jamming of the overall UMTS signal is needed. For all other operations, such as locating the phone, intercepting, etc. the target UMTS phone is either pushed back into GSM mode by the system or new UMTS Direction Finders can be supplied for locating of UMTS phones only.

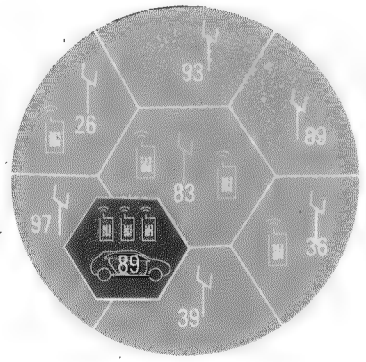
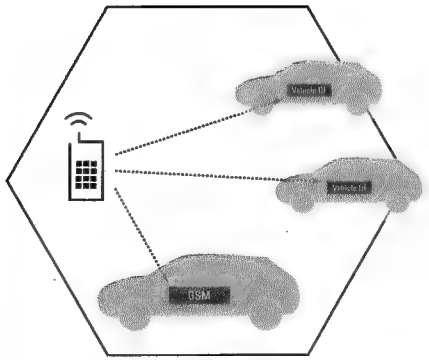



Figure: Virtual Base Station



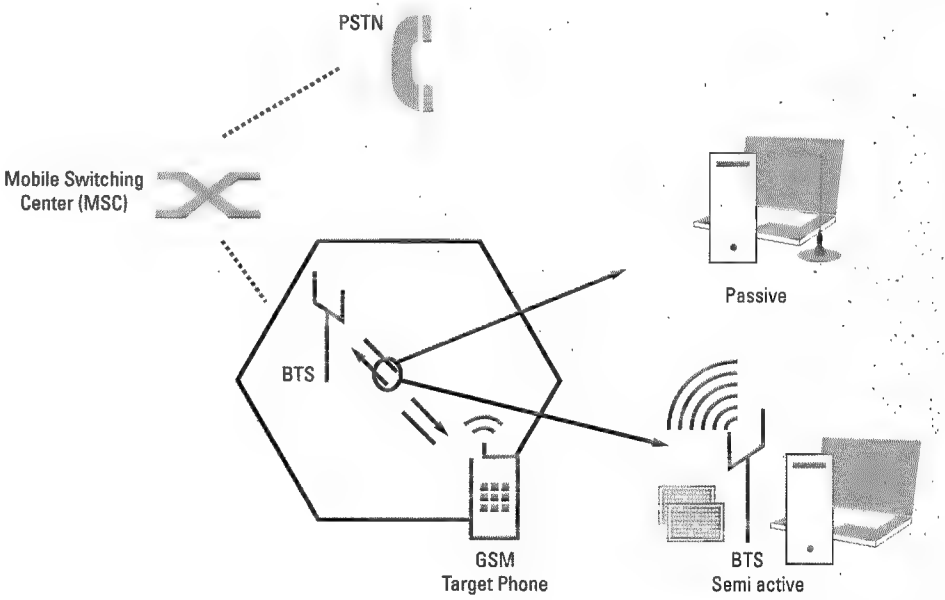

Exact locating of targets via triangulation and silent call

### Passive systems

The key function of passive off-air system is to intercept GSM phones (incoming calls and outgoing calls). The system monitors passively the air interface and therefore has no influence on transmitted numbers. The called party will always see the original calling number. Depending on the type of encryption on the air interface (5.0, 5.1, 5.2) such systems can be used and give a wide range of interception possibilities. If 5.1 encryption is used, the key must be known, otherwise 5.1 decoding systems must be available (real time decoder <1sec.) if not, then pure passive systems will not work with systems currently on the market. Passive off-air systems are portable and in combination with the use of directional antennas the range can be quite substantial (several kilometers).

### Semi Active Systems

Semi Active Systems are in place to realize GSM interception of 5.1 encrypted calls. With the active component of the system the target phone will be grabbed within milliseconds by using the 5.2 encryption mode. The 5.2 ciphering key will automatically be calculated and the authentic parameters of the target phone will be taken. These parameters are cloned onto another mobile phone (cloning box) attached to the semi active system establishing the link back to the real network (base station). The target's calls are now routed through the cloned mobile phone maintaining the same encryption, and target identity and recording for all incoming and outgoing calls is realized. Multi-channel systems are available for recording of several calls at the same time. Semi active system only work with GSM target phones having 5.2 encryption. Certain new phones only have 5.0 and 5.1 encryption available.

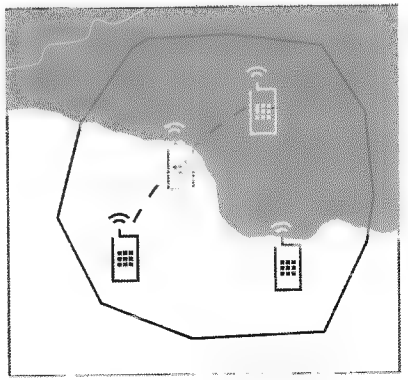


In almost every country in the world, wireless service providers are required to enable the monitoring of voice calls and data sessions, termed Lawful Interception (LI), for use by government agencies in criminal investigations and ant-terrorist measures.

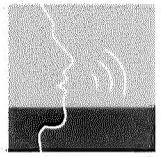
LI applications focus purely on intercepting content and have very low accuracy location context, provided by cell tower location techniques, like Cell-ID (CID) or Enhanced Cell-ID (ECID). This can render the applications ineffective because the target's actual location is relatively unknown; whereas, with accurate location data the LI mission can be accomplished with a much higher success rate. Using GPS for LI applications is not feasible because it does not work indoors and in dense urban areas, and the target user has the option to disable or jam GPS location tracking capabilities on their phone. Location technologies such as multi-lateration (U-TDOA) require radio hardware on every cell tower making it extremely cost intensive with a large degree of complexity in terms of deployment and maintenance. The solution is the only high accuracy, software-only location solution that is low cost, scalable, and reliably provides high accuracy across all types of environments. Besides high accuracy (sub 50m) and scalability, one of the key unique features of the solution is its ability to perform mass (bulk) location of all subscribers, on a near real-time basis, enabling applications such as mass location interception along with post-event analytics. The solution in conjunction with its intelligent zone services software platform also powers border zone interception with a high degree of precision.

### Key features

- **high accuracy**
- **software-only**
- **real time, historical and mass location**
- **Geo Fencing**



# SPEECH IDENTIFYING TOOLS, DATA RETENTION AND LINK ANALYSIS



The mass storage of intercepted data and its analysis is becoming more complicated and time consuming for Law Enforcement Agencies. Investigations typically involve large amounts of data gathered from a wide variety of sources (all kinds of communications monitoring systems). Somewhere in this data lies the key to an investigation, but it can remain obscured by the volume of data and the uncertainty of individual facts. Tools to filter out useless data and to visualize large amounts of data will turn the mass of information into meaningful actionable intelligence:

## Speech Identifying Tools, Analysis of Audio Data

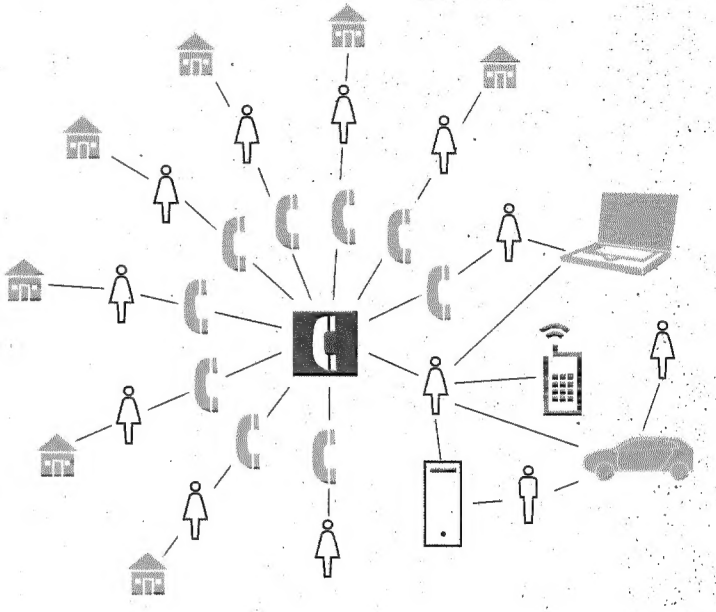
- **Speech Detection**
- **Language Identification**
- **Speaker Identification**
- **Keyword Detection**

## Data Retention

In the field of telecommunications, data retention generally refers to the storage of call related information (numbers, date, time, position, etc.) of telephony and internet traffic. The stored data is usually telephone calls made and received, emails sent and received, web-sites visited and location data. The primary objective in data retention is traffic analysis and mass surveillance. By analyzing the retained data governments can identify an individual's location, their associates and members of a group, such as political opponents.

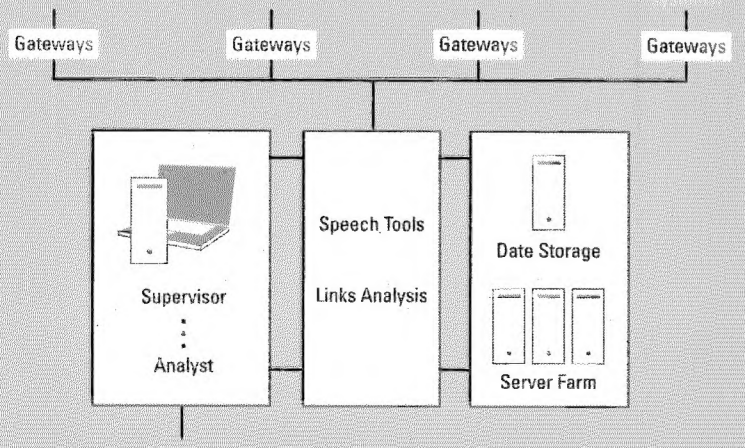
## Link Analysis

- **Visualize disparate data and turn it into meaningful information**
- **Analyze data to extract maximum value**
- **Focus on key areas**
- **Communicate the results of investigations effectively**



## INTELLIGENCE FUSION & MANAGEMENT

The collection of a huge amount of data from communications monitoring systems must be merged into one common platform to find out links between different kinds of communication targets (GSM/UMTS, Satellite, PSTN, Internet, etc.). The extraction of information for supporting decision makers and management is a central task. Intelligence Fusion system is an analysis centre for intelligence organizations, whereby highly sophisticated intelligence acquisition systems are merged. Information streams are fused and handled with one data model. Pattern recognition technology is applied (Data Retention, Link Analysis and Speech ID tools) to process unstructured information with the objective of generating additional meta data to improve analysis capabilities. Dedicated tools support the analysis and reporting process. Workflow and quality management in the intelligence back office are supported by additional dedicated tools.




## TECHNICAL CONSULTANCY FOR COMMUNICATIONS MONITORING

As part of a total service to governments and Law Enforcement Agencies, Elaman provides one of the most vital and key elements in an overall security and intelligence program – Technical Consultancy for Communications Monitoring.

More than 15 years of experience in the field of telecommunications technology allows Elaman to provide:

- **Entire technical consultancy for Lawful Interception applications for existing systems and upcoming new implementations and requirements**
- **Collecting new interception requirements and transforming those into technical specifications in order to define tender specifications and to approach and select suppliers**
- **Recommendations for technical and performance improvements and optimizing all existing Lawful Interception applications, including support for technical evaluation of offers**
- **Providing information from the market of suppliers for Monitoring/Surveillance Systems**
- **Provision of information about existing and future interception solutions for different switch vendors**
- **Consultancy in defining legal regulations for the act of lawful interception, such as in the case of privatizing the telecommunications market**
- **Works closely with clients to develop a total system solution for their needs and to ensure that they are equipped, trained and manned to meet the formidable challenges in the field of communication technology**

ELAMAN GMBH
GERMAN SECURITY SOLUTIONS

elaman
German Security Solutions

Baierbrunner Str. 15
81379 Munich / Germany
Tel: + 49 - 89 - 2 42 09 18 - 0
Fax: + 49 - 89 - 2 42 09 18 - 1
info@elaman.de
www.elaman.de